UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/714,519	11/17/2003	Simon Charles Watt	550-480	6837

23117 7590 10/17/2007

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
ABEDIN, SHANTO	
ART UNIT	**PAPER NUMBER**
2136	

MAIL DATE	DELIVERY MODE
10/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/714,519	WATT ET AL.	
	Examiner	Art Unit	
	Shanto M Z Abedin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-25 and 27-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-2, 4-25 and 27-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the communication filed on 08/02/2007.

2. Claims 1-2, 4- 25 and 27-47 are currently presented for the examination.

3. Claims 1-2, 4- 25 and 27-47 have been rejected.

Response to Amendments

4. New abstract submitted on 08/02/2007 is accepted, and previous objection to the specification is withdrawn.

Response to Arguments

5. The applicant's arguments regarding previous obvious type double patenting rejections are considered. The examiner notes, although one or more claims of the instant application might raise an issue for future obvious type double patenting rejections, previous obvious type double patenting rejections and provisional obvious type double patenting rejections are withdrawn at this time as requested by the applicant.

6. The applicant's arguments regarding the 35 USC 101 rejections of claims 24-47 are fully considered, and found persuasive, therefore, previous 35 USC 101 rejections of claims 24-47 are withdrawn.

7. The applicant's arguments regarding previous 35 USC 102 and 103 type rejections are fully considered, however, they are moot in view of newly found ground(s) of rejection (please see the office action below).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-2, 4- 25 and 27-47 are rejected under 35 USC 103 (a) as being unpatentable over Christie et al (US 7165135 B1) in view of Knight (US 2003/0126520 A1).

Regarding claims 1 and 24, Christie et al discloses apparatus/ method for processing data, said apparatus/ method comprising:

a processor operable in a plurality of modes and a plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain (Fig 1; related modes and domains; Col 4, starting at line 7, plurality of memory location associated with the plurality of the execution modes) said plurality of modes including:

at least one secure mode being a mode in said secure domain (Fig 1; related modes and domains; Col 4, starting at line 7, plurality of memory location associated with the plurality of the execution modes) ; and

at least one non-secure mode being a mode in said non-secure domain (Fig 1; related modes and domains; Col 4, starting at line 7, normal mode and domain); wherein when said processor is executing a program in a secure mode said program has access to secure data

which is not accessible when said processor is operating in a non-secure mode (Col 4, starting at line 65; Col 10, starting at line 31; Claim 1)

said processor is responsive to one or more exception conditions for triggering exception processing using an exception handler, said processor being operable to select said exception handler from among a plurality of possible exception handlers in dependence upon whether said processor is operating in said secure domain or said non-secure domain (Col 4, starting at line 7; Col 10, starting at line 31; Claim 1-9).

Christie et al fails to disclose wherein said one or more exception conditions have respective programmable configurations associated therewith that control triggering of either a non-secure exception handler operating in a non-secure mode or a secure exception handler operating in a secure mode with any change of domain also being triggered when required.

However, Knight discloses wherein said one or more exception conditions have respective programmable configurations associated there with that control triggering of either a non-secure exception handler operating in a non-secure mode or a secure exception handler operating in a secure mode with any change of domain also being triggered when required (Par 0006, 0011-0017; exception handler specific to each type of exception or interrupt).

Knight and Christie et al are analogous art because they are from the same field of endeavor of exception or interrupt handling. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teachings of Knight with Christie et al to design a method wherein said one or more exception conditions have

respective programmable configurations associated there with that control triggering of either a non-secure exception handler operating in a non-secure mode or a secure exception handler operating in a secure mode with any change of domain also being triggered when required in order to provide an efficient exception handling mechanism.

Regarding claim 2, Christie et al discloses apparatus wherein at least one of said exceptions is a selectable exception handled by a selectable one of either a non-secure exception handler operating in a non-secure mode or a secure exception handler operating in a secure mode; and at least one of said exceptions is a dedicated secure exception that is handled by a secure exception handler operating in a secure mode (Col 9, starting at line 45; Claim 2; exception handling logic).

Regarding claim 4, Christie et al discloses apparatus having a secure exception is triggered by one of a signal on a dedicated secure exception signa

Regarding claim 5, Christie et al discloses apparatus having an exception signal input shared between secure and non-secure exceptions and a further input signal cooperating with said exception signal input to control whether a secure exception handler or a non-secure exception handler is triggered (Col 9, starting at line 45; Claim 1-9).

Regarding claim 6, Christie et al discloses apparatus wherein said secure exception handler is part of a secure operating system operable in said secure mode (Col 9, starting at line 45; Claim 1-9).

Regarding claim 7, Christie et al discloses apparatus wherein said non-secure exception handler is part of a non-secure operating system operable in said non-secure mode (Col 9, starting at line 45; Claim 1-9).

Regarding claim 8, Christie et al discloses apparatus wherein said processor is also operable in a monitor mode and any switching between a secure mode and a non-secure mode required for handling of an exception takes place via said monitor mode, said processor being operable at least partially in said monitor mode to execute a monitor program to manage switching between said secure mode and said non-secure mode (Col 2, starting at line 26; Col 5, starting ln 30).

Regarding claim 9, Christie et al discloses apparatus wherein said monitor program is operable to save and restore context data defining processor status when switching between a secure mode and a non-secure mode to handle an exception (Col 2, starting at line 26; Col 5, starting at line 30; Col 10, starting at line 31).

Regarding claim 10, Christie et al discloses apparatus wherein said processor includes a register bank and said monitor program is operable to flush at least a portion of

said register bank shared between said secure mode and said non-secure mode when switching from said secure mode to said non-secure mode such that no secure data held within said register bank may pass from said secure mode to said non-secure mode other than as permitted by said monitor program (Col 7, starting at line 31; memory bank) .

Regarding claims 11 and 34, Christie et al fails to disclose wherein said exception conditions includes one of more of: a secure interrupt signal exception; a mode switching software interrupt signal; a reset exception; an interrupt signal exception; a software interrupt signal; an undefined instruction exception; a prefetch abort exception; a data abort exception; and a fast interrupt signal exception.

However, Knight discloses wherein said exception conditions includes one of more of: a secure interrupt signal exception; a mode switching software interrupt signal; a reset exception; an interrupt signal exception; a software interrupt signal; an undefined instruction exception; a pre fetch abort exception; a data abort exception; and a fast interrupt signal exception (Par 0011 to 0017).

Regarding claim 12 , Christie et al discloses apparatus wherein said processor is responsive to an exception condition to select an exception handler in dependence upon an exception vector value associated with said exception condition and stored within an active exception vector table for said exception condition; and said active exception vector table is

one of a plurality of exception vector tables (Col 9, starting at line 45; interrupt vectors; Col 9, starting at line 45; exception handling logic).

Regarding claim 13 , Christie et al discloses apparatus wherein said plurality of exception vector tables include a secure exception vector table selectable in said secure mode and a non-secure exception vector table selectable in said non-secure mode (Col 9, starting at line 45; interrupt vectors; Col 9, starting at line 45; exception handling logic).

Regarding claim 14 , Christie et al discloses apparatus wherein said processor is also operable in a monitor mode and any switching between a secure mode and a non-secure mode said plurality of exception vector is performed via said monitor mode (Col 9, starting at line 45; interrupt vectors; Col 9, starting at line 45).

Regarding claim 15, Christie et al discloses apparatus wherein said plurality of exception vector tables include a monitor mode exception vector table (Col 9, starting at line 45; interrupt vectors; Col 9, starting at line 45).

Regarding claim 16, Christie et al discloses apparatus wherein said processor is responsive to one or more parameters specifying which of said exceptions should be handled by said monitor mode exception vector table (Col 9, starting at line 45; interrupt vectors; Col 9, starting at line 45).

Regarding claim 17, Christie et al discloses apparatus wherein said secure vector table is said active vector table in said secure mode and said non-secure vector table is said active vector table in said non-secure mode unless said one or more parameters specify that said monitor mode vector table is said active vector table of said exception condition (Col 9, starting at line 45; interrupt vectors; Col 9, starting at line 45).

Regarding claim 18, Christie et al discloses apparatus wherein at least one of said parameters is stored in an exception trap mask (Col 8, starting at line 33; Col 10, starting at line 40; memory for exception/ interrupt handling).

Regarding claims 19-20 and 42-43, Christie et al discloses exception trap mask register is non-writable when said processor is not in non-secure domain (Col 3, starting at line 15; Claims 5-9; disabling debug traps).

Regarding claims 21-23,25, 27-33, 35-41 and 44-47, they recite the similar limitations that already addressed rejecting claims 1-10, 12-18 and 24, therefore, claims 21-23,25-33, 35-41 and 44-47 are rejected applying as above rejecting claims 1-10,12-18, 24.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195.

The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, AU 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

10/15/07